

ATTACHMENT B**ITEMS TO BE SEIZED**

The items to be seized are fruits, evidence, or instrumentalities of and relating to violations of 18 U.S.C. § 1512(c), Obstruction, 18 U.S.C. § 1752(a), Knowingly Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority; 40 U.S.C. §5104(e)(2), Violent Entry and Disorderly Conduct on Capitol Grounds, including:

1. Records and information that constitute evidence of identity, including but not limited to:
 - a. Clothing or gas masks worn by Thomas Robertson and Jacob Fracker at the U.S. Capitol on January 6, 2021;
 - b. flags, banners, hats, stickers, posters, and other paraphernalia;
 - c. Indicia of occupancy and ownership, including bank statements, utilities bills, vehicle registration and vehicle insurance documents.
2. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:
 - a. motive and intent for traveling to Washington, DC, on or about January 6, 2021;
 - b. plans for travel to and activity in Washington, DC, on or about January 6, 2021;
 - c. mode of travel, travel expenses, and travel logistics on or about January 6, 2021;
 - d. activities in and around Washington, DC on or about January 6, 2021;
 - e. Plans to travel to Washington, DC, or Richmond, Virginia, between January 6, 2021, and the present.
3. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Thomas Robertson or Jacob Fracker about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.
4. Evidence of participation in extremist groups involved in the planning of the January 6, 2021, attacks on the U.S. Capitol.
5. Property or records from the U.S. Capitol.
6. Computers and/or electronic storage media including all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers. A “storage medium” for

purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include, but are not limited to, external hard drives, CDs, DVDs and flash drives.

7. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the “Device(s)”:

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- e. evidence of the times the Device(s) was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. records of or information about Internet Protocol addresses used by the Device(s);
- i. records of or information about the Device(s)’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.